IN THE CLAIMS:

Please amend claims 1, 22, 25, and 27 as follows:

1.   (Currently Amended) A method for managing at least one server using remote intelligent mail messages, the method comprising:

receiving, by a mail agent, an electronic mail message, sent by a user, requesting a service relevant to a <u>hardware component of</u> at least one server;

deciphering the electronic mail message to understand the nature of the service requested by the user;

determining whether the user has a privilege to obtain the service; and

performing the service, by the mail agent, if the user has the privilege, to produce a service outcome.

2.   (Original) The method according to claim 1, wherein the mail agent runs on one of the at least one server.

3.   (Original) The method according to claim 1, wherein the electronic mail message includes an encrypted electronic mail message.

4.   (Original) The method according to claim 1, wherein the user belongs to at least one category of a set of categories.

5.   (Original) The method according to claim 4, wherein the at least one category includes a category of server administrators having a complete information access privilege.

6.   (Original) The method according to claim 4, wherein the at least one category includes a category of users having an access privilege to view information only.

7.   (Original) The method according to claim 1, wherein the user sends the electronic mail message from a client.

2

8.	(Original) The method according to claim 7, wherein the client includes one of a remote computer, a cellular phone, and a wireless handheld device.

9.	(Original) The method according to claim 1, wherein the deciphering comprises parsing the electronic mail message.

10.	(Original) The method according to claim 9, further comprising decrypting the electronic mail message, if the electronic mail message is sent encrypted.

11.	(Original) The method according to claim 1, wherein the determining comprises:

examining the security credentials of the electronic mail message;

authenticating the user;

verifying the access privilege of the user based on an access control list stored in the server; and

deciding whether the user has the privilege for the service based on results from the examining, the authenticating, and the verifying.

12.	(Original) The method according to claim 1, wherein the service includes inquiring as to health information of the at least one server.

13.	(Original) The method according to claim 12, wherein the health information includes memory usage.

14.	(Original) The method according to claim 12, wherein the performing comprises:

contacting at least one server to which the service pertains;

obtaining the health information from each server that is contacted by the contacting; and

generating the service outcome by composing a health information report based on the health information obtained by the obtaining.

3

15.   (Original) The method according to claim 1, wherein the service includes taking at least one action on the at least one server.

16.   (Original) The method according to claim 15, wherein the action includes a reboot.

17.   (Original) The method according to claim 15, wherein the performing comprises:

connecting to at least one server to which the service pertains;

executing the at least one action on the at least one server;

determining the effect of the at least one action on the at least one server; and

generating the service outcome based on the effect, determined by the determining.

18.   (Original) The method according to claim 1, further comprising:

generating a return electronic mail message based on the service outcome; and

sending the return electronic mail message to the user as a reply to the requesting a service.

19.   (Original) The method according to claim 18, further comprising encrypting the return electronic mail message prior to the sending.

20.   (Original) A method for managing at least one server using remote intelligent mail messages, the method comprising:

obtaining, from at least one server health monitoring system, health information about at least one server;

generating a first electronic mail message using the health information;

sending, by a mail agent, the first electronic mail message to a user;

receiving, by the mail agent, a second electronic mail message, sent by the user, requesting a service relevant to the at least one server;

4

deciphering the second electronic mail message to understand the nature of the service requested by the user;

determining whether the user has a privilege to obtain the service; and

performing the service, by the mail agent, if the user has the privilege for the service.

21. (Original) The method of claim 20, wherein the first electronic mail message is generated by the mail agent.

22. (Currently Amended) A system for managing a server using remote intelligent mail messages, the system comprising:

a server;

a client configured to allow a user to send electronic mail; and

a mail agent configured to communicate with the server and the client, the mail agent being further configured to receive an electronic mail message, sent by the user from the client, requesting a service relevant to a hardware component of the server, decipher the electronic mail message to understand the nature of the service requested by the user, and perform the service to produce a service outcome.

23. (Original) The system of claim 22, wherein the mail agent runs on the server.

24. (Original) The system of claim 22, wherein the client includes one of a remote computer, a cellular phone, and a wireless handheld device.

25. (Currently Amended) A mail agent for managing at least one server using remote intelligent mail messages, the mail agent comprising:

a mail handler configured to receive an electronic mail message, sent by a user, requesting a service relevant to a hardware component of the at least one server;

5

a deciphering mechanism configured to decipher the electronic mail message to understand the nature of the service requested by the user;

a privilege determination mechanism configured to determine whether the user has a privilege to obtain the service; and

a service performance mechanism configured to perform the service, if the user has the privilege, to produce a service outcome.

26.   (Original) The mail agent of claim 25, further comprising a decryption mechanism configured to decrypt the electronic mail message if the electronic mail message is sent encrypted.

27.   (Currently Amended) A computer-readable medium encoded with a plurality of processor-executable instructions for:

receiving, by a mail agent, an electronic mail message, sent by a user, requesting a service relevant to <u>a hardware component of</u> the at least one server;

deciphering the electronic mail message to understand the nature of the service requested by the user;

determining whether the user has a privilege to obtain the service; and

performing the service, by the mail agent, if the user has the privilege, to produce a service outcome.

28.   (Original) The computer-readable medium of claim 26, wherein the deciphering comprises parsing the electronic mail message.

29.   (Original) A computer-readable medium encoded with a plurality of processor-executable instructions for:

6

obtaining, from at least one server health monitoring system, health information about at least one server;

generating a first electronic mail message using the health information;

sending, by a mail agent, the first electronic mail message to a user;

receiving, by the mail agent, a second electronic mail message, sent by the user, requesting a service relevant to the at least one server;

deciphering the second electronic mail message to understand the nature of the service requested by the user;

determining whether the user has a privilege to obtain the service; and

performing the service, by the mail agent, if the user has the privilege for the service.

30.   (Original) The computer-readable medium of claim 29, wherein the first electronic mail message is generated by the mail agent.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /